Privacy and Security Tiger Team
Draft Transcript
November 12, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody and welcome to the Privacy and Security Tiger Team. This is a Federal Advisory Committee and there will be opportunities at the end of the call for the public to make comments. Just a reminder, workgroup members please remember to state your name.

Deven McGraw, are you on?

Deven McGraw – Center for Democracy & Technology – Director
I am.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – Software Entrepreneur
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Gayle Harrell?

Gayle Harrell – Florida – Former State Legislator
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Carol Diamond?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Judy Faulkner? Carl Dvorak? David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Neil Calman? David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi? Rachel Block? Alice Brown?

Alice Brown – National Partnership for Women & Families – Director HITP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel? Leslie Francis? Adam Greene?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anybody off?

Deven McGraw – Center for Democracy & Technology – Director
And Leslie didn't say "here" but she might have been on mute. We know we had her on.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes, I had her. Okay, I'll turn it over to Deven and Paul.

Paul Egerman – Software Entrepreneur
Thank you very much. This is Paul Egerman. I appreciate everybody's continued dedication to be on the call on a Friday afternoon. This is the Privacy and Security Tiger Team and we are meeting this afternoon to try to see if we can complete our discussion of an interesting issue, it may seem a little arcane, this issue of provider entity authentication.

This is a discussion about what kind of digital credentials and what are the basic policy guardrails for issuing digital credentials that allow one computer to talk to another computer. We had a list of six questions, which we posted on the HIT Policy Committee's blog, the FACA blog. We got a huge amount of responses, which were really very helpful, and we're going to be talking a little about those responses. But I would tell you, I happened to be in D.C. earlier this week at a different meeting of the Enrollment Workgroup, and a member of the public walked up to me, ... Michael DeCarlo was his name, and he said he had been listening to all of our meetings and actually made some comments. So I do want to thank any members of the public who may be listening in to our call. I certainly also want to thank all the members of the public who put forward the very useful comments, which, as you will see, are definitely influencing our discussion.

So where we are going to take our discussion right now, again, is we have six questions. We went through the first four of them in our previous call and what we would like to do is to continue on. So I'm going to quickly advance the slides past the four that we've already done to question number five. Also to make sure that everybody understands the timing of what we're trying to accomplish is a week from today on February 19th the HIT Policy Committee is having its regular monthly meeting. What we'd ideally like to be able to do, if possible, if we can get a consensus, is to complete our discussion on this topic of provider entity authentication and present it to the Policy Committee, hopefully in the form of a recommendation and put that in front of the Policy Committee for consideration for approval or perhaps feedback. That's our schedule.

Before I launch into question number five, do you have any comments, Deven, or does any member of the Tiger Team want to say anything?

Deven McGraw – Center for Democracy & Technology – Director

The only thing I want to add is that, again, our aim is to try to get through these questions. The slides that we have circulated had the earlier questions and encompassed the discussion that we had initially, so our hope is to get through the rest of them. Then what we'll do is I'm going to raise a couple of issues that I noticed in the public comments that I think are worth teeing up further and then hopefully we'll be able to do all that within our time period here.

Paul Egerman – Software Entrepreneur
Sounds good.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
What's the format that this is going to go to the Policy Committee in, in terms of presentation, or how is it going to be presented?

Paul Egerman – Software Entrepreneur
Deven and I, before this call, were actually just talking about that. Probably what we'll do is we'll put it in the format of a PowerPoint presentation and depending on the feedback we get following the presentation turn it into a transmittal letter.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
The reason why I ask that question is because having just gotten off a couple of hours conference call with the Governance Workgroup, I just want to make sure that somewhere at the beginning of ... present this, that it's clear that this is not intended to step on or circumvent what the Governance Committee is doing. Because there are a lot of areas that if you listen in on both sets of calls you'd probably say my God there's some overlap, and I think we just want to make sure that we navigate this so it's clear that we're really not trying to solve each other's problems but try to work—

Paul Egerman – Software Entrepreneur
You, John, are on the Governance Committee, is that right?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That's correct. There are areas where when you read through these questions and comments that you could interpret it to mean that we're doing the same thing.

Paul Egerman – Software Entrepreneur
Again, that's a helpful comment. The reason why we wanted people on multiple committees is so that they can help us coordinate and find out when we're accidentally stepping on each other's areas, so a very helpful comment. Any other comments?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
No, thanks.

Paul Egerman – Software Entrepreneur
Also one administrative thing before we launch into these questions, one of the pieces of feedback we got back from the public is to ask all of the participants to, again, say your name before you start speaking. I think we've been on the phone together enough that we're starting to recognize each other's voices pretty frequently, but we want to make sure that the public who is taking the time to listen in also can understand who is speaking. So please say your name before you talk.

Question number five, we broke this into two questions. Actually I'm going to look at 5a and 5b together; 5a says: "Should ONC select an established technology standard for digital credentials?" 5b says: "Should EHR certification include the criteria that tests capabilities to communicate using that standard?" So the reason for looking at 5a and 5b together is, and it seems to me if you're going to develop a standard there's no reason to develop a standard unless you're also going to do certification. If you want to do certification around this you have to do this standard. The question is, should we have a standard

and also should we have certification? That's what we need to decide. The possibilities are yes, establish a standard, and yes, do certification and testing around it. The other possibility would be to say no, don't do that. In the public comments we actually got both reactions. Some people said, "Yes, you should do this," and some people said, "No, let the industry do whatever they want." My question to you is, what's our answer to this?

Deven McGraw – Center for Democracy & Technology – Director
Before we launch into this, can I ask a question? The question is really directed at those of you on the phone who are on our technology expertise side. That is, one of the reasons why it's necessary to select the standard versus just requiring that a particular technical functionality exists would be because you need it in order for systems to be interoperable. If you think about one of the recommendations that we've already put on the table, which is that there would be multiple credentialing, multiple entities to issue digital credentials, do they all need to be issuing it in some way that's interoperable or is it sufficient that they just be issuing those credentials in accordance with our policies? I don't know the answer to the question. It's not a hypothetical one for me.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'll get us started. I think the question is simpler than it probably needs to be because there are multiple layers on which one could have both a combination of standard and non-standard activity. So I'll just relate to you, for example, the experience with direct and indirect, or direct connect, in building out the privacy ensuring mechanism for those direct conversations we put together something that has never been put together before but we did it completely out of standard building blocks. You'd be hard pressed to say it's a standard, but you'd also be hard pressed to say that there's anything in there that isn't standard. It's the way we put the building blocks together that was slightly unique even though the building blocks themselves are all based on well established standards. So I don't know that that helps the conversation. It just means to me that it may be overly simple, but I think I would lean in the direction of saying that the industry should be allowed to assemble well understood technologies in ways that don't require a start from scratch approach to security.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think it's pretty clear that the credentials have got to be standard because they'll be read by a machine, and machines are not smart. They're going to be anticipating certain fields. They're going to be anticipating that the content in those fields will be captured in a particular way. So essentially I think the credentials must be standard and I think the federal government is the right one to establish that standard. What I mean is the structure of the credentials, what fields are mandatory and the way that information is captured in those fields, those two things have to be standard. Deven, you mentioned how they're distributed. That doesn't have to be standard, but what a machine anticipates receiving must be standard.

Paul Egerman – Software Entrepreneur
Dixie, that's very helpful. I want to also ask you as it relates to the next question, by saying it should be standard are you also saying that there should be certification criteria?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Absolutely, because the EHR will need to receive this credential and authenticate the individual based on it. So that EHR has got to be tested to make sure that it can do that.

Paul Egerman – Software Entrepreneur
So the concept would be pretty much as you just said, that if you established a standard and if you said that there should be certification around it, what that would mean would be for some transactions, or perhaps all transactions, the vendor would have to prove that they do this, that they have a certificate established that they send and they check the certificate at the other end that they're doing it with the correct technology.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. For stage one meaningful use where we don't have a requirement for digital signatures, the certification criteria would only be looking to see that they can use that certificate to authenticate the endpoints of the transactions. Then I suspect that later on, I'm anticipating stage three or possibly stage two, eventually EHRs will have to also be able to handle the credentials for digital signatures as well. But for stage one it should just be being able to use a standard and an X509 or whatever credential to authenticate the two endpoints.

Paul Egerman – Software Entrepreneur
Okay. So your answer to this question 5a is yes, and your answer to the next question is yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, it is.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Let me, with great trepidation, debate Dixie. I know better than to argue with Dixie, but I think perhaps we're actually not disagreeing. When I talk about standardized, I'm thinking in terms of plug-and-play interfaces that just connect up and go. I certainly agree with Dixie's point that the credential mechanism, PKI 509, whatever, should be standardized. What I was talking about that might be more variable is the way in which those credentials are shared and communicated and the way they're used actually to protect the message or to protect the transmission. You can use those digital credentials over SOAP. You can use them over RIS. You can use them over SSL. Those are all not interoperable with each other even though they're all using the same standard credentials. So that's what I meant by the question needs to be maybe slightly more precise, but at the level of the credential I think it would be standard.

Paul Egerman – Software Entrepreneur
If I understand you correctly, I think there's not any inconsistency with what Dixie is saying.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Absolutely not. I totally agree with him. The question says standard for digital credentials, not for the exchange of digital credentials.

Paul Egerman – Software Entrepreneur
Right. Because the way I'm looking at it there's almost like three different concepts. There's the credential. There's what I call the transport standard, the transport methodology, and then there's the content standard or the content methodologies. Those are three different things.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I disagree. I think transport's different. But the credential, you've got to look at the structure of it, which fields need to be populated as well as what the contents have to look like within the—

Paul Egerman – Software Entrepreneur
The contents of the credential?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – Software Entrepreneur
Okay. That's fine. When I talked about content I was thinking more about what I think NHIN direct calls the payload, the actual content of the transaction. So maybe I need a better word for that. So the three concepts are the credential, the transport technology, and the payload. Those are the three separate—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
... will include content itself, like when it expires—

Paul Egerman – Software Entrepreneur
That's correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
... and that has to be captured in a standard way or the EHRs can't interpret it.

Paul Egerman – Software Entrepreneur
Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The word that threw me on the slide was the word "interoperable." I think I was leaning towards the notion of interoperability at the level of the full transaction, which would include all of those layers. Whereas, Paul, I think you're addressing a question more towards the credential itself.

Paul Egerman – Software Entrepreneur
Yes, that's what I was trying to do. I'm trying to say, and I'm probably not saying it correctly, I'm trying to say there are multiple layers and that this is just one of the layers.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, and I'm with Dixie—

Paul Egerman – Software Entrepreneur
... standardize this layer knowing that that by itself doesn't by itself create interoperability but by itself it's like a step forward to help you create interoperability, because it's one component.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right, and it's a critical component obviously because it has to do with identity and security. I agree with Dixie. I think we're comfortable that the certificates need to be standardized. I'm sorry, the credentials, we're using the word "credentials" not certificates.

Paul Egerman – Software Entrepreneur
Yes, because I was also under the impression, and you have to tell me if I've got this right, David, that actually in terms of standards themselves there's not that many to choose from. There's some ... within them in terms of how you set it up, but—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
David has pointed out a really good point. In that question it really should be technology standards for digital certificates. Credentials are what you present to get a digital certificate.

Paul Egerman – Software Entrepreneur
I see.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, that's a good point.

Paul Egerman – Software Entrepreneur
... terminology.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's probably why I slipped back into saying "certificate." I think you're right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, you're right.

Paul Egerman – Software Entrepreneur
Dixie, that's probably my mistake, my fault. So the correct terminology is talking about digital certificates, and credentials is like your application form?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, how you prove that you are who you are.

Paul Egerman – Software Entrepreneur
Okay, I apologize for screwing that up. It seems the two of you are saying yes in agreement. Are there any other comments? Does anybody disagree?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think we're having a love fest here. I think it's—

Paul Egerman – Software Entrepreneur
Yes—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is one of the easier things I think we've talked about.

Paul Egerman – Software Entrepreneur
Yes. You have to excuse me, John. It's so different for me to hear so much equanimity. It's like I don't know what to do next, so I'm dragging it out and enjoying it. But what I should do next is go on to the next question.

M
We should go find—

W
... suggestion.

M
We should try to go find Wes and have somebody to spice it up.

Paul Egerman – Software Entrepreneur
This is good, because this is really a critical point. This is really critically important and I think we made good progress. This is question six, which is I think if I remember correctly Neil Calman asked is really what types of questions must be authenticated.

W
And is there a permanent level of assurance.

Paul Egerman – Software Entrepreneur
Right. The types of questions, so there are some things written here, patient risk or PHI, both transactions. Another way one can answer it is whatever are the meaningful use exchange transactions should be authenticated. What answer do people think is appropriate for this question?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would say that any transaction where the identity of the sender and/or receiver needs to be assured and/or the information exchange needs to be protected has to be authenticated.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That makes sense to me. I think to come up with a counterexample, someone who is just seeking information from, say, an HIE about HIE policies could do so with a Web browser and not be authenticated because there's no risky information at stake. But if they were in fact interacting with the HIE to upload or download or query patient data, then obviously that would have to be authenticated and credentialed and protected.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
The one bust to that is the question do you do it on a transaction by transaction basis, or do you do it on a connection by connection basis and once you've determined that the connection is valid, if there are multiple transactions that might stream over that connection such as a large provider might do, would you assume that all those transactions within a stream are then credentialed?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Now you're getting to the nature of the transaction. But in most cases it will probably be authenticating the two ends and then establishing a trusted, encrypted path between them to create a virtual session.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That's to my point. Because I think what I heard some of this was that every transaction needed to be credentialed. What you're saying is no, as long as you develop a trusted relationship, as long as a trusted relationship exists, then you don't have to worry about re-credentialing.

Paul Egerman – Software Entrepreneur
That would be my expectation also. To do a simple example, if you're a laboratory and you want to send a stream of laboratory results, you may want to send 100 patients, you may want to send 1,000 results at once, because you have them all ready. One would think you should be able to authenticate, do some sort of handshake to make sure that everything's correct and then send the entire stream.

Deven McGraw – Center for Democracy & Technology – Director
I think that makes sense, Paul. But I actually thought what John was asking is if you have authenticated that handshake at the onset of your relationship and then establish a trusted, whether it's a virtual private network or some other mechanism for communicating from that point forward, do you need to continue to authenticate past that point? So in your lab example, yes, of course you've authenticated you said the thousand transactions or you said one, and then a week later when you send some more transactions do you need to re-authenticate? I thought that was what the question was, but maybe I misjudged.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, you have to re-authenticate with every session.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

Paul Egerman – Software Entrepreneur
Yes, I think that's correct, although, Dixie, isn't that part of what I call the transport technology? Doesn't the description—?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, not at all. You use the transport to connect it to the spot, but you authenticate the endpoints and then the transport carries the data between it. Then you encrypt over the transport once you've authenticated the two endpoints, but you can easily have a transport without authentication or anything.

Paul Egerman – Software Entrepreneur
Okay. So, John, is your question answered? Are you comfortable with this?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Yes, I think so. Yes, I think we're all on the same page.

Paul Egerman – Software Entrepreneur
So getting back to the question then, Dixie has proposed a response which is any transaction where it's important to know the identity of the sender or receiver or if the information that is being included in the transaction needs protection. So it's a fairly broad description of the transactions, and if I heard correctly, David said he agreed with that. So my question is, are there any other comments? Is that the correct answer to the first part of this question or ... or comments on that?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Paul, would you repeat it one more time? I got ... and didn't hear it ....

Paul Egerman – Software Entrepreneur
Dixie will correct me when I make a mistake, I hope. Any transaction when the identity of the sender or receiver is important to validate or if the information within the transaction needs protection.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would also make it clear that in some cases you might need to authenticate one end and not the other and in other cases you might have to authenticate both ends. For example, if you were connecting to an HIE and you really wanted to make sure that that's who you're connecting to but they may not necessarily have to know who you are, you may just be going in but you want to make sure that the information that you get there is from that HIE, then you might want to authenticate that HIE but not necessarily the person coming in.

Paul Egerman – Software Entrepreneur
That's a good observation, Dixie. I do want to remind everybody, the question that we're trying to answer right now, the first part is what type of transactions must be authenticated.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I just think we should say and/or.

Paul Egerman – Software Entrepreneur
When you say and/or, and/or where?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
In that sentence that you read, where the—

Paul Egerman – Software Entrepreneur
The sender and/or, okay, the receiver needs to be known. Okay, so we have this broad statement that Dixie is putting forward which sort of says any transaction where it's important to do this, then you should do it.

M
That's a little bit of a ....

Paul Egerman – Software Entrepreneur
Say again?

M
I said it's a little bit of a topology. It's a self-defining statement, a self-referential statement. I think the question is probably, so what does that mean? What kind of transactions need to be protected? I think the list you've got there, certainly patient risk or PHI would be in the list. I think transactions that would be authenticated outside of health care like, for example, financial transactions, if such things were happening, that probably would be on there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think it's—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
... anyway.

Paul Egerman – Software Entrepreneur
I'm sorry. Somebody just said something.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
A financial transaction would in some ways have PHI associated with it anyway.

Paul Egerman – Software Entrepreneur
That's right.

M
Yes, most likely, yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think it's dangerous to try to make a list.

Paul Egerman – Software Entrepreneur
Dixie, I think you're probably right, but it probably is helpful to list some examples.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Examples, I agree.

Paul Egerman – Software Entrepreneur
Because otherwise we may not be telling anybody anything, and so I think to list these as examples is good. What about saying, is it a good idea or not a good idea to say, well every information exchange that's described in meaningful use?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
There you go.

Deven McGraw – Center for Democracy & Technology – Director
Yes, that's a good example. Did I hear Rachel in the background?

Paul Egerman – Software Entrepreneur
Was somebody speaking?

W
It was Gayle.

Paul Egerman – Software Entrepreneur
Gayle, I can barely hear you. Can you—?

Gayle Harrell – Florida – Former State Legislator
This is Gayle.

Paul Egerman – Software Entrepreneur
Now I can hear you. Thank you.

Gayle Harrell – Florida – Former State Legislator
I think we have to go back to the basic Paul Tang premise in which any transaction that information may be divulged or where a patient may be surprised to find out that somehow that information went to an entity or goes through something and it's not authenticated, I think you need to go back to what the information is, what it involves, and would the patient be surprised to know that.

Paul Egerman – Software Entrepreneur
So you're saying another criteria, because any transaction where a patient expectation would be that the transaction would be protected.

Gayle Harrell – Florida – Former State Legislator
Correct.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I'm not sure I'd give a lot of guidance, though.

Paul Egerman – Software Entrepreneur
I'm sorry. Was somebody trying to speak?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
It doesn't really give us much more guidance than what we're talking about. I think this is the difficulty here, the Justice Potter issue, "I can't define pornography but I know it when I see it." We all in our sense of things know that there are things that are sensitive that we need to worry about credentialing against, but I think it's almost infinite what it could be.

Gayle Harrell – Florida – Former State Legislator
I think you're going to have to give some specific examples to make people understand what we're talking about.

Paul Egerman – Software Entrepreneur
I agree. The question I have for Gayle and John is, what about specifically the information exchange transactions that are described in meaningful use.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think that's a great example. I think there are a lot of others too. I agree. I just want to make sure we're very clear that this is not an all-encompassing list, because I think that there will be so many people asking for exceptions and what about this and what about that.

Paul Egerman – Software Entrepreneur
If we say "the information exchange transactions described in meaningful use," then we've also said something very concrete that the certification people can use. So every transaction that's in meaningful use then gets certification criteria written against it. So if meaningful use says you have to do a patient summary with a CCD or with a CCR format, then it would be tested with the ability to be transmitted against a digital certificate.

Gayle Harrell – Florida – Former State Legislator
However, things such as financial information and insurance information and things of that sort also could be transmitted and we don't have any requirements for that in stage one meaningful use.

Paul Egerman – Software Entrepreneur
That's right. I meant it though as a specific concrete example.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Another bullet.

Paul Egerman – Software Entrepreneur
In other words, I didn't mean it to be limiting. If we say that, that will give us a mechanism to do testing. I agree with what you're saying, though, because financial transactions fall within the category that you described and that Dixie described, but we should probably simply list them as a separate example, so claims eligibility, we can very simply list them out. Pardon me?

Gayle Harrell – Florida – Former State Legislator
PHI covers all of those.

Paul Egerman – Software Entrepreneur
I agree.

Gayle Harrell – Florida – Former State Legislator
It doesn't have to have health data in it in order for it to be PHI. It just has to have identifiers in it, then it's PHI.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's true. The other point that I think we should make sure we cover is safety critical information that may not have any patient identifiers in it at all. For an example, if you're retrieving a clinical guideline, for example, you should authenticate where you're getting the clinical guideline.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Are clinical guidelines going to be standardized, or are those things that people will be able to establish ad hoc by themselves?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Mostly providers have a lot of their own clinical guidelines, but anything that would affect how you treat the patient or if you're even downloading an upgrade to your software, any of those things that could affect really how your system works or how you're going to deliver care to the patient should always be authenticated.

Deven McGraw – Center for Democracy & Technology – Director
Dixie, if I do a Medline search, do I have to authenticate to Medline if ... search? But if I'm doing so in the process of figuring out how to treat somebody—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes—

Deven McGraw – Center for Democracy & Technology – Director
... how to authenticate for that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I once mentioned this at one of the hearings that we had in the Standards Committee that years ago I did a penetration activity that demonstrated that I could go in to a certain place and change the provider's treatment guideline. So you really need to authenticate who comes in and changes them as well as who you're retrieving them from so they will affect how you deliver care, even though they're not patient specific.

M
But it's an asymmetric ... at the exchange. You need to know that they are valid, but they don't need to know who you are.

Paul Egerman – Software Entrepreneur

That's right. It's also an issue that what you call a treatment guideline is not PHI.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's right. That's my example. I don't think everything that needs to be authenticated necessarily contains PHI.

Paul Egerman – Software Entrepreneur
I agree.

Deven McGraw – Center for Democracy & Technology – Director
I'm not disagreeing either, but I feel like we're straying into some territory just for the purpose of listing an example that I'm not sure I fully understand.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's why I don't think we should list examples, because as John said, people are going to always question your examples.

Paul Egerman – Software Entrepreneur
Let me make two comments. One is, I think we need to stay focused on information exchange. I think the digital certificates can be used for other purposes, but information exchange is really exchange of information between providers. It's—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's not necessarily PHI information. It can be clinical information. Suppose you got an e-mail from a provider that suggested—

Deven McGraw – Center for Democracy & Technology – Director
I get it, Dixie. I think, though, our purpose in listing examples is not to provide a broad universe, but to make sure that people understand for the transactions that are of most concern to us, which is the exchange of data for meaningful use, those would certainly be included. I think given the broad recommendation that you described, which I think is a good one, providing a couple of examples that are not a mutually exclusive list is not a bad idea. But I don't think that means we have to list every other possible one. My discomfort with straying into the territory that you're raising is that we just don't know enough about that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, I'm fine with that as long as we still have our umbrellas.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
So it seems like we have a consensus about a description of the transactions, where this consensus, on the second bullet it says "both transactions," and Dixie did a great job of describing this concept that you can authenticate sessions. There's also this other comment at the end about a common level of assurance and the bullet on this screen says under the authentication at the organizational level that a single level of assurance seemed appropriate. Does anybody want to comment on that?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
We have examples in the DEA ruling on ePrescribing for non-uniform levels of assurance, so the level of authentication and certainty required for regular prescriptions is different from controlled substances. Whether that's a model that we should pay attention to or not, certainly it's out there and it's kind of a new thing for health care.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Good point, very good point.

Paul Egerman – Software Entrepreneur
So your comment is we already have circumstances where there's some additional level of assurance that is being required for certain transactions, so maybe that's a good precedent, to simply say this is a baseline and under some circumstances other levels of authentication may be necessary.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, I think so. I think it would be hard to say no, uniform is fine in the face of a clear example where it's not.

Deven McGraw – Center for Democracy & Technology – Director
Yes, we're not trying to undermine the DEA standard, right?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think the DEA example is an excellent example and I think it's one of the reasons why we should express to the state that the model needs to accommodate multiple levels and types of authentication.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we should make it just real, since we're talking about certification of EHRs we should make it just very explicit that an EHR must support both single factor and two factor authentications.

Paul Egerman – Software Entrepreneur
We're talking about it at an entity level, Dixie, not about—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I thought this was going in the EHR certification?

Paul Egerman – Software Entrepreneur
It is. But right now we're just doing information exchange as part of the—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's the same thing. I'm still talking about organizations too, but just put that it has to be able to support ... and leave the policy of exactly when that will be sort of open.

Paul Egerman – Software Entrepreneur
How do you support two factors on an organizational basis?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't know.

Paul Egerman – Software Entrepreneur
I understand two factors when you're talking about individuals, but I don't understand it when two computers talk to each other.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's a good point. We really are talking about level of assurance of the credential issuing and the credential management process rather than the actual transactions.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Then the DEA example doesn't apply, because that's really prescribing and you don't prescribe at an organization level either.

Paul Egerman – Software Entrepreneur
That's right.

Deven McGraw – Center for Democracy & Technology – Director
That's right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, that's a good point. It's not organizational, but it is multi-level individual.

Paul Egerman – Software Entrepreneur
That's right. We're not talking about the individuals yet. We're going to talk in a few minutes about the individuals. Right now we're just trying to get the computers to talk to each other.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's a good point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we need to make that clear in our question, Paul, because when you present it this topic will come up again.

Paul Egerman – Software Entrepreneur
Yes, and so it's sort of like a repeat of what we did even on question one, the common level of assurance question at an organizational level it's like a square peg in a round hole. It doesn't quite fit the structure that we're talking about here.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw – Center for Democracy & Technology – Director
I think we want a level of assurance that all organizations – at the beginning we wanted to have some pretty high assurance that the organization is who they said it was, but that didn't necessarily translate into the customary levels of assurance that people apply at the individual user level.

Paul Egerman – Software Entrepreneur
I agree, Deven. It seems to me, though, unless I've been hearing otherwise, it feels to me like we've answered question six. Describe the transactions, we said yes on both transactions. Under the third bullet about single level and multi-factor we're reminded of when we're talking about organizational level and responding to it in the context of saying we've got to have the right amount of proof that the organization is who they say they are.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's right, yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Once you decide that the organization has a certain amount of proof, then you have to rely upon the organization to ensure that its individual users then are properly authenticated by the organization and that ... information's appropriate.

Paul Egerman – Software Entrepreneur
That's a great comment, John, because it sort of segues into what we want to talk about next. Deven, if we're comfortable with our answers ... I think Deven wants to review some of the comments that we received from the public on the blog and what you just said, John, about future authentication was certainly a recurrent .... Before I turn the call over to Deven, because she's going to review the public

comments and take us back through a few of the questions, is everybody comfortable with question six, with the way I've summarized this?

W
Yes.

Paul Egerman – Software Entrepreneur
Okay. So, Deven, why don't you take us through the questions? First, let me to just say this is great progress that we managed to get through all six of these questions. I think we have some very good concepts here, so I'm very excited about these answers. Go ahead, Deven.

Deven McGraw – Center for Democracy & Technology – Director
I want to go back, and it looks like I can do that, which is great. What I did after our last call was to go back through not just the comments that the MITRE team, who helps us so much had summarized for us on our last call, but because we extended the time of the comments many of the comments that came in in that additional week there wasn't time to get them in the summary. I just wanted to make sure that we had a way to double-check and make sure that we were listening to the people who had bothered to comment on us and taking what they commented on under consideration.

So I'm taking us back to 2b, where we had a discussion on our last call about what an organization seeking digital credentials would need to demonstrate. We really focused on are you an organization? Do you actually exist? Are you participating in a health care transaction? In our world of health information exchange, to get a digital credential you should be doing something health care related, and particularly tied to what's necessary for the meaningful use providers to be able to accomplish meaningful use. Then we also said that organizations who perform this credentialing really ought to rely on existing criteria and processes when those are applicable. One of the examples that we talked about was the national provider identifier, because that is actually a pretty rigorous process that those providers who need to get them have to go through, and that provides a reliable point, a reliable set of credentials that could essentially be relied on.

We got a lot of comments, I wouldn't say that everybody commented on this, but we got a fair number of comments from people who wanted organizations seeking digital credentials to have to either agree to or demonstrate that they comply with some set of privacy and security criteria, so whether this is compliance with law. Whether this is compliance with a set of criteria that are similar to those that you would find in the DURSA, which is the agreement that entities that are participating in NHIN exchange, and I think also NHIN Connect have to sign, but it's at least through NHIN exchange, it's a data use and reciprocal support agreement which sets out some very clear rules of the road for entities exchanging in NHIN exchange. There were a number of people who thought that there ought to be some similar criteria applied to digital credentials in this space.

Now, commenters who said we didn't need to put any additional criteria other than proof of organizational existence and being involved in health care essentially reminded us that we have a lot of other mechanisms for making sure that people comply with privacy and security. The lobbying one, and there are a number of others that are in consideration, certainly the Governance Workgroup is exploring governance mechanisms for holding people accountable to best practices. Similarly we've been doing some thinking in the Meaningful Use Group about whether there ought to be meaningful use criteria along these lines, we have certified EHRs that are required to include certain functionalities. So their advice to us was this is not the appropriate place for a policy lever. We've got other policy levers. This should really be something that gets used to ensure that machines can talk to one another. We shouldn't try to load this down with the burden of being another law enforcer or another policy enforcer. So I wanted to get the Tiger Team's thoughts on whether we want to add to these requirements, as some people suggest, or leave them as is and rely on other policy levers to accomplish the good privacy and security practices and compliance with law that we want and see what you all thought.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Deven, I really do believe that the Governance Committee is handling a lot of that. I would agree that there are other levers that are going to, I think, ... measure address this.

Gayle Harrell – Florida – Former State Legislator
Could we possibly, on our next call, get some idea as to where the Governance Group is and what some of those things are that they're proposing or the levers that you're talking about would be to perhaps give us a little higher degree of security on this.

Deven McGraw – Center for Democracy & Technology – Director
That's a good idea, Gayle. I think they are also in some pretty intense phone calls to try to tee up some recommendations for us at the Policy Committee. Is that right, John?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That is correct. There's a lot of calls being scheduled but we're really very much on the same trajectory in terms of our thoughts on what I think you're talking about here.

Mary Jo Deering – ONC – Senior Policy Advisor
I have been lurking. We'd be happy to arrange that. In any case, I think we certainly want to go in to the Policy Committee meeting looking like we've been talking to each other. So we'd be happy to—

W
That would be good.

Paul Egerman – Software Entrepreneur
Although, Mary Jo, the next meeting of this group is on November 22nd, after the next Policy meeting.

Mary Jo Deering – ONC – Senior Policy Advisor
Okay. We can certainly brief you at that point on where they're at if people haven't been able to hear it at the Policy Committee meeting.

Paul Egerman – Software Entrepreneur
It would be helpful, you might want to get the chairs, Deven and me and the chairs of the Governance Committee into a call before November 19th to make sure that we're coordinating our presentations.

Mary Jo Deering – ONC – Senior Policy Advisor
Excellent idea.

Deven McGraw – Center for Democracy & Technology – Director
But in the meantime, if people are leaning towards John's point, that there are other and better hopefully governance vehicles for assuring compliance with privacy and security laws and best practices, we can always put that as a placeholder and make that assumption, that we know that governance is working on this. So we're going to look to that, we're going to rely on that process unless as we sort of meld these efforts a little better together we find that we're not satisfied with that, we can take it up again.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is—

Mary Jo Deering – ONC – Senior Policy Advisor
They'll be getting into the validation issues next week. They haven't begun to touch on those in detail. It may well be that they don't get to a level that you're looking at and so I would think that that might be a potential disconnect.

Deven McGraw – Center for Democracy & Technology – Director

John, you were saying something?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I was just going to say I don't see a disconnect at the level we're talking about. But I also would say that probably one of the things we want to do is make sure that Deven and Paul speak with John and that if in fact John agrees, which I think he's going to, as to why we split this up, then I think you can go further and say that through coordination with the Governance Committee that these topics will be addressed by the Governance Committee, so that there's an explicit hand-off.

Paul Egerman – Software Entrepreneur
I think what you just said, John, makes sense. The other comment I want to make that is perhaps something that we have to make in our presentation is that we cannot view these digital certificates as like the sole basis of security. We shouldn't look at the process of issuing a certificate like that's our only methodology to create security for this network. There has to be other mechanisms. This is just one component.

Deven McGraw – Center for Democracy & Technology – Director
Yes, that's absolutely right. We said that in our assumptions slides in the earlier meeting and we'll have to make sure that we make sure we're clear to the Policy Committee on that as well.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'm comfortable with focusing really on identity and transaction security, but not on the behaviors of the other organization. I think it's a slippery slope that you could end up certifying that they follow evidence-based medicine or something. It's hard to know where to draw the line, so I think we should stay away from it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Is the Governance Workgroup considering some method of certifying, or some other word that means about the same thing, credentialing organizations?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes, I think that's all part of the dialogue is exactly how do we ensure that organizations are appropriately credentialed before they participate.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
... the people who issue the certificates, the organizations that actually issue the certificates. Because if we put some simple rules down here it really all comes down to the integrity and trustworthiness of the organization that issues the certificates to begin with.

Paul Egerman – Software Entrepreneur
Right. It's a good comment, because that's an issue that actually already exists, it's my understanding that it exists. Sometimes the organization that issued digital certificates didn't necessarily do such a great job. But one of the recommendations we made was that there be some accreditation process for that, an accreditor, and so that might be ONC itself or it might be an organization that ONC identifies to accredit the credentialing issuing organizations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree with that completely. Who made that recommendation?

Deven McGraw – Center for Democracy & Technology – Director
We did.

Paul Egerman – Software Entrepreneur
We did.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We did?

Deven McGraw – Center for Democracy & Technology – Director
Yes, I just went to it on the slides. It's part of recommendation four, question four's answers.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

Paul Egerman – Software Entrepreneur
The basic structure here is similar to what we do in certification. With certification we said there could be multiple entities that could certify EHR systems, but there needed to be one accreditor that monitors those organizations. So this is like the same recommendation. There can be multiple entities that issue the digital certificates but there needs to be an accreditor organization, either ONC itself or somebody that ONC identifies who views them to make sure that it occurs correctly.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I must have nodded off. I apologize.

Paul Egerman – Software Entrepreneur
Dixie, there's no need for an apology. This is such impressive, riveting, exciting information that no one could possibly nod off.

Leslie Francis – NCVHS – Co-Chair
Paul, it's also an unfair trade practice to say that you're living up to a standard when you're not.

Deven McGraw – Center for Democracy & Technology – Director
Yes, it is.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, good.

Paul Egerman – Software Entrepreneur
That's a good point.

Deven McGraw – Center for Democracy & Technology – Director
It sounds like we've got, I'll just go back to 2b for a second because that's where we were. So it sounds like we are comfortable with the recommendation as is because we believe that, at least at this stage, that the Governance Workgroup is working on an accountability process that is the preferred vehicle for assuring accountability for privacy and security, both practices. That's the gist I'm getting. I think I'm in agreement with that. I think that's the right way to go. I just want to make sure that we've heard from everybody on this issue.

Gayle Harrell – Florida – Former State Legislator
The only thing I would add to it is that when you do the presentation that you make sure that we name that and identify that, that we are doing the hand-off to the Governance Group. We expect a certain level to come back from the Governance Group, but we are cognizant of people's feelings on this.

Deven McGraw – Center for Democracy & Technology – Director
I think you're right, Gayle, and I know that they're struggling with how to do this because these are not easy questions. I think the Policy Committee will be getting recommendations both from us and from them. Ideally, we try to coordinate those as best as possible, but if we find that there's a more lightweight set of governance recommendations than we're expecting, I personally don't think that it's likely to

happen, but if it is we certainly, I think, if we think that there are some of our recommendations that need an accountability mechanism that is somehow stronger than that, then maybe we'll have to do something at that point. I think at this phase when there's so much that's uncertain that isn't all on our plate we need to accommodate that.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
My apologies, I have to go, but thank you all for your hard work.

Deven McGraw – Center for Democracy & Technology – Director
Thank you, John. Thanks for joining us. You've had a lot of phone calls with ONC today.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes. You have a great weekend. Thank you very much.

Deven McGraw – Center for Democracy & Technology – Director
Thanks, you too.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
....

Deven McGraw – Center for Democracy & Technology – Director
Yes, you've got to go too, Carol. Thank you.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Thanks.

Leslie Francis – NCVHS – Co-Chair
Deven, another way to put what you just said is that we don't need to have two people doing the same thing with respect to privacy, or two committees. But we need to make sure it's done and if Governance doesn't do it then the hand-off has to come back.

Deven McGraw – Center for Democracy & Technology – Director
That's another good way to put it. Any other thoughts before we go on to the next— I have one more topic to raise from the comments. All right, well, we'll go to that.

Another set of comments that I wanted to bring to your attention are whether we need to, in some future set of meetings, because we wouldn't be able to do this in the time that we have available to us today, deal with a set of policy recommendations down at the individual user level. In all of our recommendations it's very clear that they are directed at provider entities, the machine to machine handshake, making sure that the organization is who it says it is and creating a policy infrastructure for that. We did get some comments, well, we got a lot of comments from folks who were confused about what we were doing, but among some of the commenters who recognized that we were doing entity authentication and not authentication of individual users within entities, a number of them said in order to create the trust framework for exchange you're going to need to have policies down at the individual user level—

Paul Egerman – Software Entrepreneur
For user—

Deven McGraw – Center for Democracy & Technology – Director
For user authentication, right, or else you won't be able to do that. I know this is a very difficult question and in a second I'm going to pause and let Paul share his comments, because we did have some discussion about that this week. On the one hand, I can sympathize with the views of folks who urged us to go down this road because from a general perspective the trust framework is only going to be as strong

as its weakest link and if you've got organizations who satisfy entity level credentialing but have crappy or sloppy identification and authentication of their individual users it's going to weaken the trust framework.

On the other hand, setting some general policies with respect to individual users in a health care system that has such widely varying resources, levels of expertise, I think is going to be really tough to do. We already have the HIPAA security standard, and Dixie will of course correct me if I don't have this right, does set some general guidelines. We've known all along that providers are responsible for the security within their entities, and that includes that they need to have policies with respect to identifying and giving access to the individual users of their systems, but I don't think it's quite at the level where some people were urging us to go. So I think the question for us to discuss here is not to get down into the details of what those policies would look like for individual users, but I think whether we think this needs to have a national set of policy recommendations beyond what the law already requires. If that's the case I think we would then try to schedule it for a later discussion.

Paul, I'm going to stop and defer to you, because I want to make sure that you have a chance to share views from our conversation, and then we'll open it up to the Tiger Team.

Paul Egerman – Software Entrepreneur
I'll just say that user authentication is a complicated issue. Having said that, I'd rather just open it up and ask for feedback from the Tiger Team members. Do we want to try to attack that issue? John Houston mentioned it before he left as an issue, so what do people think? ... user authentication.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that a generic statement somewhere that says systems which have been authenticated at the entity level must ensure that their users are properly authenticated when they are accessing these services that have been authenticated at the entity level, and leave it as kind of a broad statement but not try to get completely specific. Because I think, for example, if one of the authenticating entities is an EMR that's connecting, for example, to a local HIE, you might have different standards, say, than a PHR where you have consumers authenticating into the PHR. So I think it definitely needs to be mentioned, but I'm not sure we want to dive into the specifics of each kind of entity.

Paul Egerman – Software Entrepreneur
So you're saying broad statement and not to try to dive into it?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, basically. I think for the specific cases for meaningful use, at least with respect to the EHR, EMR, we already have certification criteria around access control and user authentication and I don't think we want to try to revisit that. Now, for non-EMR users it may not be so clear.

Leslie Francis – NCVHS – Co-Chair
This might be another place to in some respects punt it to Governance, because if we don't want to say there's a common standard, what we do want to say, picking up on the weakest link point, is that this is a situation in which you have to be really sure that people are doing security right. So unless there's some kind of appropriate oversight to be really sure that people are doing security right, then there has to be a ... national standard.

Gayle Harrell – Florida – Former State Legislator
I'd like to jump in on it also. I think that if we punt it to Governance, then we need to have some real good sense of where they're going, because this is where the public gets very nervous. When you have a large entity with multiple people using a system and you're down, this is where things happen, you get down to that individual level and the entity needs to have a certain responsibility and the governance needs to be there to make sure that they are doing what they need to do. The patients and the public get very nervous at this point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think for us to make any statement at all about authentication within an organization is inappropriate, because we have to assume individual authentication is a HIPAA requirement. It's not one of these addressable ones. It's required that every organization must authenticate each individual user, must assign a unique identifier to each individual user, and we have the Office of Civil Rights that is supposed to be clamping down on enforcement of HIPAA but for us to step forward and say well you must individually authenticate, that is certainly at the very least repetitive of what HIPAA already requires. So I would not say a thing about authenticating users inside an organization. I think, if anything, we might want to consider whether there are any meaningful use transaction stage ones that are critical enough that at the network level, at that organization to organization level you still want to have accountability at an individual level. My—

Paul Egerman – Software Entrepreneur
Dixie, that's a good issue, but it's a different issue.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But I don't think it's appropriate for us to look inside an organization at all.

Paul Egerman – Software Entrepreneur
Okay, so I just want to stick with that issue. Does anybody want to say that they disagree, that we should be doing that?

Leslie Francis – NCVHS – Co-Chair
I don't want to say that we should be doing that, but we should be saying at the ... levels that it's absolutely important that that be done right within each organization that talks to each other.

Paul Egerman – Software Entrepreneur
That's helpful, because that's similar to something I thought I heard David say. So I'm trying to understand, what precisely should we be saying?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think we should say anything.

Paul Egerman – Software Entrepreneur
Dixie, you're saying say nothing.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right.

Leslie Francis – NCVHS – Co-Chair
I think we should be saying that there needs to be very good governance standards to be sure that people are meeting up with the appropriate HIPAA authentication standards. We shouldn't be prescribing anything more about what those standards should be, this is Leslie, but we should be saying at the level above what the actual authentication methods are that there needs to be really good oversight mechanisms because this can be very risky business fast.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Which is also required by HIPAA.

Leslie Francis – NCVHS – Co-Chair
But you want to make sure that HIPAA's being followed, that's all I'm saying.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I know, but that is also required by HIPAA. The majority of the requirements in HIPAA are not technical requirements, they're oversight governance requirements.

Paul Egerman – Software Entrepreneur
Dixie, could you just explain why you think we should be silent on this issue? Is it because it's already in HIPAA? Why should we be silent?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Because it's required by law, it's already required by HIPAA, they're already required to do risk assessment, they're already required to do audit reviews, and they're already required to have strong oversight of HIPAA compliance within their organization. HIPAA has three areas, the HIPAA security standard I'm talking about. It has administrative requirements, physical security requirements, administrative security, physical security, and technical, and the vast majority of the requirements are these administrative requirements to oversee to make sure that security is being maintained. I think us saying anything is saying we don't think people are following HIPAA.

Leslie Francis – NCVHS – Co-Chair
I think I'm up a level, because I'm not saying what's within organizations, administrative or technical or whatever safeguards there should be, but I'm saying that at the level of oversight, whether it's the Office for Civil Rights or whatever, that's the level that I take governance to be talking about, ... within organizations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
ARRA strengthened that. Before ARRA the Office of Civil Rights had oversight only for the privacy rule and now they have oversight for both the privacy rule and the security rule, so the governance is also there.

Deven McGraw – Center for Democracy & Technology – Director
So here's the thing, I think that we should not assume that the Governance Workgroup is limiting their scope just to things that are above and beyond the law. Rather than saying, I think it's absolutely clear, at least from the discussion of folks who have talked so far, that we're not interested in pursuing additional substantive requirements here. We think the substantive requirements are taken care of in the law. What we're now discussing is, is there room for some accountability beyond the regulators just doing their job and enforcing the law? To me that seems like it's straying into territory that the Governance Workgroup may or should, depending on your viewpoint, be handling and we ought to leave to the side until we know a little bit more details about what that proposal is going to look like and what its scope will be, whether anything additional on the accountability mechanism needs to occur. I don't—

Gayle Harrell – Florida – Former State Legislator
I'd like to make a comment here. I think it's important again for public perception reasons that we reiterate that recommendation, that we do look to Governance to examine that and to look very carefully to make sure that we feel that HIPAA and the Office of Civil Rights offer mechanisms that are already there that are handling that. I think it's important to make the public statements within our recommendations and acknowledge that we are giving that responsibility off to Governance.

Paul Egerman – Software Entrepreneur
That's very helpful. So thinking about what you just said and thinking about what Dixie said, the sense I have is that we understand that the certificates are not the sole basis of security and that HIPAA compliance in general and user authentication in particular are extremely important and we want to remind everyone of the importance, the work by the Governance Committee to review all of these areas.

Leslie Francis – NCVHS – Co-Chair
What I think we're saying is that our answer to the second question that Deven raised is exactly parallel to our answer for the first question.

Deven McGraw – Center for Democracy & Technology – Director
That's right.

Paul Egerman – Software Entrepreneur
Plus to Governance.

Deven McGraw – Center for Democracy & Technology – Director
That's right.

Gayle Harrell – Florida – Former State Legislator
And that Governance is very important here and that if it were to turn out that we're not satisfied with what they say on that point we might want to come back.

Paul Egerman – Software Entrepreneur
As I hear what Gayle said, she's saying that it's really very important in our presentation that we mention this.

Gayle Harrell – Florida – Former State Legislator
Exactly. I believe it is.

Deven McGraw – Center for Democracy & Technology – Director
I agree with her. Well, those were the two issues that I wanted to bring up, although one of the points that Dixie made earlier about whether certification for EHRs ought to accommodate more than one factor authentication, if an entity chooses to use it for its individual users, would this be the space to talk about that or is that something that Dixie, you would want to work on with your standard Privacy and Security Workgroup?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Whichever way you want to go is fine with me. We really aren't having regular meetings there. I don't know.

Deven McGraw – Center for Democracy & Technology – Director
Okay. It seems to me that certainly the EHRs ought to be able to accommodate whatever level of policy the organizations choose to implement.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, there is one area, but the standards and certification criteria obviously follow the stage one meaningful use, right, and we had a lot of discussion about authentication mechanisms and EHRs ... even for the first recommendation. So right now there are no specific recommendations beyond what HIPAA already requires, but as David pointed out earlier, at the EHR level is where that new DEA regulation is going to kick in, so eventually we're going to have to put in place a standard and security and certification criteria for two factor authentication of EHRs.

Deven McGraw – Center for Democracy & Technology – Director
Right, that makes sense. Yes, that makes sense.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
May I bring up something? I was just looking at HIPAA kind of relating to our last conversation, I just noticed there's a whole HIPAA requirement, and administrative requirements about the standard has to do with information access management, and the implementation specification for access authorization, which has to do with deciding who gets an account and what privileges they have, as well as access establishment and modifications, which is when you decide they need higher or lower or need to be changed, or when they leave a company you take their account off, both of those are addressable instead

of required. Now, if we wanted to do anything with respect to strengthening what they did with authentication and access management within an organization we might recommend that those be made required.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Dixie, I think the most relevant provision here is actually the technical safeguards, which is under "D, Person or Entity Authentication."

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And that's required, right.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Right, that's required. As a technical safeguard they must implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right. But our group was just talking about strengthening the assurance associated with that and the assurance is decisions made from an operational perspective on who gets the accounts to begin with. You might have really strong authentication, but if Alice can give her daughter an account if she wants to, then you don't have much protection.

Deven McGraw – Center for Democracy & Technology – Director
Here's my suggestion, is that rather than signal to the Policy Committee that we're taking on the issue of individual user authentication next, because I thought we got some pretty clear indication that folks didn't think it was necessary to go in that direction given a whole host of factors. But certainly we have an entire security bucket of issues that we want to take on in the future at some point in 2011 and that we need to put a book marker on the one that you've just raised, Dixie, and think about it when we get to that discussion. Does that make sense?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That makes complete sense, yes.

Deven McGraw – Center for Democracy & Technology – Director
Okay, so it sounds like we've resolved the two issues that I raised in quite similar ways, as Leslie aptly pointed out. Paul, unless I've forgotten one that you thought I was bringing up, I think we've got a good set of recommendations.

Paul Egerman – Software Entrepreneur
Yes, I think we do too. It also shows the value of getting the public feedback too, because it did cause us to re-look at our recommendations and think through a number of very important issues. Before we open the call to public feedback, let me ask, do any members of the Tiger Team have any other things they want to talk about or anything they would like to say?

Deven McGraw – Center for Democracy & Technology – Director
Before we do that, Paul, I just want to let folks know that the MITRE team helps us, takes notes during this call, as do I, but they take much better notes than I do. We're going to revise these slides in accordance with the discussion that we had today and get them back out to you. We don't have time for another call, so this is just for you guys to eyeball, keep us on our toes, and if you've got wordsmithing suggestions you want to push to us, it will be a very short turnaround that we'll give you probably, you'll get them either late Monday or early Tuesday. But again we don't have any further calls but I think we've got a good set of recommendations. But I did want to let you know that we will pass by you the slides that we intend to present to the Policy Committee for one last look.

Paul Egerman – Software Entrepreneur

Yes, that's correct. Thank you.

Deven McGraw – Center for Democracy & Technology – Director
Sorry, that was all I had to say.

Paul Egerman – Software Entrepreneur
Okay. Not hearing that anybody has anything else to say, Judy, why don't we open it up for public comment?

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes, let's invite the public to see if anybody has a comment. Operator, could you please inquire?

W
... Friday afternoon.

Judy Sparrow – Office of the National Coordinator – Executive Director
I know. Well, you all got a lot done, though. It was a good call.

W
We need to have more Friday afternoon calls.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes.

Operator
You have a public comment.

Dr. Don Berman – Digital Renaissance Group
This is Dr. Don Berman from the Digital Renaissance Group. I have been listening quite enraptured to this whole program, because I just went to one the other day which addressed the HITECH Act, which pretty much covers what you need to protect as far as the list you were referring to with concern. And your comments regarding the two factor authentication or identifying the users, as well as the devices which are accessing the system, because you have to recognize that digital certificates are on devices but anybody can walk up to the device and utilize it.

The comments regarding an absolute identification of the user is right on target because that's exactly what you need to do, and I commend you for that. But I want you to be aware of, if you aren't already, that there are smart cards which are widely vetted and in use by the federal government which do exactly that, the carrier of the card can be biometrically identified so that he then can access the device with that digital certificate on it. So you've got two factor authentication with existing programs that are federally vetted, and I just want to say that I think you are really right on target with both of those approaches.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great, thank you very much. Any other comments?

Operator
We do not have any more public comments.

Paul Egerman – Software Entrepreneur
Terrific. I just want to thank the Tiger Team for their dedication on a Friday afternoon. I want to thank our good friends from MITRE for all their help, and of course ONC and Judy Sparrow.

Deven McGraw – Center for Democracy & Technology – Director
And Adam from OCR.

Paul Egerman – Software Entrepreneur
Of course, Adam, from OCR, you are the best. You're always extremely helpful. You always seem to have the answer, so we really appreciate your help.

Deven McGraw – Center for Democracy & Technology – Director
Thank you, everyone.

Paul Egerman – Software Entrepreneur
Thank you very much. Have a very good weekend.

Deven McGraw – Center for Democracy & Technology – Director
Have a good weekend.

Public Comment Received During the Meeting

1. I thought the discussion was about authentication of entity connections. Where does the transaction come into this in Q 6? Once a connection has been authenticated and allowed to take place then the authentication process being discussed is finished. There may be another discussion regarding authentication of transactions.